

AIR WAR COLLEGE

AIR UNIVERSITY

SUN TZU IN CYBERSPACE

by

Scott W. Rizer, Lt Col, USAF

A Research Report Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements

16 December 2008

DISCLAIMER

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE DEC 2008		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Sun Tzu in Cyberspace				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air War College, Maxwell Air Force Base, Alabama				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 48	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Introduction.....	1
Background	2
Cyberspace	2
Definitions	3
Cyberspace Domain and Information Operations	3
Cyberspace Characteristics.....	4
Sun Tzu	5
Interpretation	5
Taking Whole	6
<i>Shih</i>	8
<i>Tao</i>	9
Supporting Principles	11
Analysis.....	14
Cyber Attack	15
Relative Decisiveness	15
Capabilities Mix	17
Cyber Attack Effectiveness	22
Cyber Exploitation	23
Contribution to <i>Shih</i>	23
Levels of War	24
Collection Means and Subject.....	24
National Security Role	25
Cyber Defense	26
Defensive Adaptation	27
Two-Model Defense.....	28
Conclusions.....	34
Bibliography	37

Illustrations

	<i>Page</i>
Figure 1. Cyberspace/Sun Tzu Strategy Model	14

INTRODUCTION

This paper asks how cyberspace capabilities will most likely contribute to strategy. The cyberspace domain, much as the arrival of the air domain before it, provides a mix of known and unknown strengths, weaknesses, opportunities and threats. Cyberspace is often treated as transformational or exceptional relative to other domains and its evolution challenges current assumptions regarding organizational roles and responsibilities, doctrine, tactics, techniques, and procedures both inside and outside the Department of Defense. All of these issues are being addressed in a simultaneous and iterative manner as the collective understanding of the cyberspace domain matures.

This paper is based on the premise that strategy provides the conceptual foundation for most of these issues. Considering how cyberspace capabilities contribute to strategy provides insight into the ultimate question – to what purpose do we operate in cyberspace? This, in turn, provides direction for further research into future technologies, organizational constructs, roles, responsibilities, tactics, techniques and procedures. Sun Tzu's *The Art of War* provides a useful analytical framework for answering this question because its timeless and conceptual nature is not tied to a specific environment or context. With Sun Tzu as a guide, this paper takes a skeptical position towards cyberspace's exceptionalism relative to the experience of other domains and instead argues that an effective way to look to the future is to learn from the past. As Michael Handel notes, "Ultimately, the logic and rational direction of war are universal and

there is no such thing as an exclusively ‘Western’ or ‘Eastern’ approach to politics and strategy; there is only an effective or ineffective, rational or irrational manifestation of politics or strategy.”¹

The Background section provides definitions, concepts and supporting principles for cyberspace and *The Art of War*. The Analysis section integrates the *Art of War*’s concepts on strategy with the characteristics of cyberspace and is organized along the core cyberspace capabilities of attack, exploitation and defense. The Conclusion section provides a summary of the main conclusions that will be derived from the analysis.

BACKGROUND

Cyberspace, an emerging warfighting domain comprised of advanced networking and communications capabilities is oriented towards the future. In contrast, Sun Tzu’s *The Art of War* was authored over two thousand years ago in a distant land and foreign culture. Both topics justify deep and broad backgrounds that would easily exceed the constraints of this paper. Consequently, this background focuses on the concepts that directly support its analysis, conclusions and recommendations and admittedly omits significant subjects.

Cyberspace. This cyberspace background: a) provides definitions, b) distinguishes the cyberspace domain from its capabilities such as information operations, and c) presents key characteristics that distinguish it from the traditional warfighting domains.

¹ Handel, *Masters of War*, 3.

Definitions. Defining cyberspace has been a challenge because it can be alternatively perceived as the physical nodes (servers, computers, wires) that make up the global information grid, the physical information (zeros and ones) contained in the grid or the cognitive meaning that information has for decision makers. The National Military Strategy for Cyberspace Operations focused on cyberspace's physical attributes and defines it as, "A domain characterized by the use of electronics and electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."² This definition has been adopted by DOD and serves as a sound theoretical foundation for distinguishing what cyberspace is from what it isn't. Key to that distinction is separating the concept of cyberspace as a physical domain from the capabilities and missions that occur in the domain due to the cross functionality of cyberspace capabilities and the cross-domain characteristic of information operations.

Cyberspace Domain and Information Operations. Cyberspace capabilities are cross functional and are not limited information operations. Lt Col Fahrenkrug reinforces this distinction saying the Air Force intends to, "...create very real effects in cyberspace that affect the adversary's ability to orient his forces, command and control, or even fire weapons. These are not effects that simply occur in the adversary's mind. In other words, these are not virtual or imagined effects – the adversary can in fact die or be harmed through warfighting in cyberspace."³ Similarly, information operations are cross-domain activities and are not limited to cyberspace. "When viewed from the perspective of a warfighting domain, cyber operations

² Fahrenkrug, *Cyberspace Defined*.

³ Ibid.

will improve our efforts to influence our adversaries and others using information operations in all the domains.”⁴

Cyberspace Characteristics. Cyberspace has unique characteristics that distinguish it from other warfighting domains and impact its role in strategy. First, although cyberspace architectures are physical our presence in cyberspace is virtual so while we can never physically be in cyberspace our presence can “be” in adversarial cyberspace with an immediacy and 24-7 persistence that are difficult to achieve in other domains. This leads to two cyberspace access characteristics that are related but opposite in their effects: a) lack of sanctuary and b) lack of forced entry.

There is no sanctuary in cyberspace because access is potentially available wherever cyberspace exists. Once an element is networked it is a component of cyberspace and exists as a potential warfighting domain. “As a realm of operations, the infosphere or cyberspace exhibits peculiarities and properties; despite having a real topology, it has no geography. Physical distances or separations become meaningless; as a result, there are no ‘denied areas’ but also no ‘sanctuary’ in this domain.”⁵ Although there is no sanctuary in cyberspace, likewise there is no forced entry into cyberspace.⁶ Cyberspace can only be entered where opportunities already exist. Whether through the exploitation of a password or unknown system vulnerabilities intruders can

⁴ Fahrenkrug, *Cyberspace Defined*.

⁵ Cooper, *Another View of Information Warfare: Conflict in the Information Age*, 128.

⁶ Libicki, *Conquest in Cyberspace*, 39.

only enter cyberspace where the means exists. “Hackers have little extant ability to create entry paths – only to exploit them.”⁷

Cyberspace also provides few barriers to entry which enables a broader range of threatening actors than traditional domains. “One can place the threat agents executing these attacks into four profiles: hackers, organized crime, terrorists, and nation states.”⁸ Convertino, DeMattei and Knierim list several attributes that can make cyberspace an attractive attack option including the broad span of physical and informational effects, surgical precision, stealth and low probability of detection, attribution and traceability.”⁹ Combined, these attributes provide very real advantages to cyber attack and very real challenges to cyber defense.

Sun Tzu. *The Art of War* describes basic concepts and principles of strategy while leaving the details of how to apply them to the reader. As Ralph Sawyer notes, “Over the millennia the book’s concepts have stimulated intense debate and vehement philosophical discussion, commanding the attention of significant figures in all realms.”¹⁰ Although Sun Tzu’s concepts can be characterized as timeless this background begins with a cautionary note due to the challenges of interpreting a writing that is thousands of years old and presented through metaphors and analogies. Then it presents the following core concepts from *The Art of War*: a) limiting costs and risks by taking whole, b) *Shih*, c) *Tao* and d) the supporting principles of initiative, knowledge, deception, surprise, flexibility and creativity.

⁷ Libicki, *Conquest in Cyberspace*, 39.

⁸ Convertino, DeMattei and Knierim, *Flying and Fighting in Cyberspace*, 23.

⁹ Ibid., 42-43.

¹⁰ Sawyer, *The Art of War*, 79

Interpretation. Interpreting and understanding *The Art of War* can be challenging due to the distance in time and culture between its writing and today's environment. Some, like James Adams, have asserted that *The Art of War* may be unintelligible to the Western mind, "... Sun Tzu's writings were the external manifestation of a complete and deeply rooted philosophy on life that a Westerner can only dimly comprehend."¹¹ Roger Ames counters that the cross-cultural nature of interpreting *The Art of War* presents both advantages and disadvantages and ultimately concludes, "In pursuit of understanding, we have no choice but to attempt to identify and excavate these uncommon assumptions ..."¹²

Another challenge to interpreting *The Art of War* is its use of analogies and metaphors to develop broad concepts and supporting principles. While principles provide, "an adopted rule or method for application in action,"¹³ Sun Tzu's concepts provide, "an idea of something formed by mentally combining all its characteristics or particulars ..."¹⁴ which requires study, thought and analysis. The book, "...does not develop its doctrines through logical demonstration. Rather, it teaches by analogy and metaphor. We cannot simply pluck its insights and drop them into our already existing frameworks. We must develop new ways to use our minds."¹⁵ Ultimately, some of Sun Tzu's most important concepts are not explicitly stated and must be derived through analysis. This is a potential weakness because it is subject to misinterpretation but it is also a potential strength because it is timeless.

¹¹ Adams, *The Next World War*, 256.

¹² Ames, *The Art of Warfare*, 45.

¹³ Dictionary.com., "principle" definition 6.

¹⁴ Dictionary.com., "concept" definition 2.

¹⁵ Denma Group, *The Art of War*, xix.

Taking Whole. The *Art of War*'s first important concept is the importance of limiting risks and reducing costs or of "taking whole." According to Sun Tzu, warfare must be studied because the existence of the state could literally depend on it. Mistakes could not only be costly, they could prove fatal. In Sun Tzu's time, "...warfare had evolved sufficiently to endanger the existence of virtually every state, large and small alike. Many had already perished; innumerable ruling families had been extinguished and their peoples subjugated; and others tenuously survived only through adroit political maneuvering and servile submission."¹⁶ Thus, *The Art of War*'s opening lines read, "War is a vital matter of state. It is a field upon which life or death is determined and the road that leads to either survival or ruin, and must be examined with the greatest care."¹⁷

All translations of *The Art of War* note the priority Sun Tzu places on victory with the lowest cost and risk. The Denma Group refer to this concept as "taking whole." According to their interpretation, "Taking whole means conquering the enemy in a way that keeps as much intact as possible - both our own resources and those of our opponent."¹⁸ They are quick to point out that this importance is based on calculations of cost and risk. "This is not merely a philosophical stance or altruistic approach. Destruction leaves only destruction, not just for those defeated, their dwellings and their earth, but also for conquerors."¹⁹ Other interpreters similarly note the importance of winning without fighting to avoid risk and loss. "Warfare always constitutes a loss. As the Sun-Tzu observes, 'If one is not fully cognizant of the evils of

¹⁶ Sawyer, *The Art of War*, 128.

¹⁷ Ames, *The Art of Warfare*, 103.

¹⁸ Denma Group, *The Art of War*, xvii.

¹⁹ *Ibid.*, xvii.

waging war, he cannot be fully cognizant, either, of how to turn it to best account' ... even military victory is 'defeat' in the sense that it requires an expenditure of a state's manpower and resources."²⁰ Sawyer elaborates on this important theme as well. "Whenever possible, 'victory' should be achieved through diplomatic coercion, thwarting the enemy's plans and alliances, and frustrating his strategy. Only if the enemy threatens the state with military action or refuses to acquiesce without being brutally forced into submission should the government resort to armed combat."²¹

When fighting proves unavoidable strategy should be guided by those same priorities. According to Ames, "The first priority is the avoidance of warfare if at all possible. Once, however, a commitment has been made to a military course of action, the project becomes to achieve victory at the minimum cost."²² Likewise, Sawyer notes, "... every military campaign should focus upon achieving maximum results with minimum risk and exposure, limiting as far as possible the destruction to be inflicted and suffered, fighting with the aim of preservation."²³ The vital importance of preserving oneself and avoiding risk and loss is reinforced throughout *The Art of War* and provides the philosophical basis for strategy and the concepts that follow.

Shih. Sun Tzu develops the important concept of *Shih* through analogies and metaphors that require interpretation. Ames refers to *Shih* as "strategic advantage"²⁴ and describes it as, "... the full concentrated release of that latent energy inherent in one's position, physical and

²⁰ Ames, *The Art of Warfare*, 85.

²¹ Sawyer, *The Art of War*, 129.

²² Ames, *The Art of Warfare*, 85.

²³ Sawyer, *The Art of War*, 129.

²⁴ Ames, *The Art of Warfare*, 104.

otherwise.”²⁵ The Denma Group agree on the positional nature of *Shih* and describe it is a function of relationships, “*Shih*, then, is like looking at a chessboard: the effectiveness of a position is read in terms of the relative power of certain pieces, the strength of their formation, their relationship to the opponent, and also their potential to turn into something else.”²⁶ But, they also elaborate on the analogy by observing, “The world is more complex than three- or even five-dimensional chess ... and there’s a further crucial notion, which is timing; the right moment to step in, to take the shot, to release the accumulated energy.”²⁷ This leads to Sawyer’s interpretation of *Shih*, which is the most succinct. Sawyer begins with the analogy of tumbling stones and notes that the force they deliver depends equally on their course towards a target (position) and their mass and momentum (power). “Thus it appears that two equally important factors are integrated by this concept ... first, the strategic advantage conveyed by superior position, and second, the power of the forces involved ... accordingly we have chosen to translate the term *Shih* by ‘strategic configuration of power’”²⁸ Sun Tzu presents *Shih* through many analogies such as a hawk striking its prey in flight, cascades of water flowing through a gorge and the potential energy of a bow and arrow. All serve to demonstrate the importance of the strategic combination of superior power and superior position in space and time. These configurations, however, are changing and fleeting. The fluid nature of *Shih* leads to another of Sun Tzu’s concepts – *Tao*.

²⁵ Ames, *The Art of Warfare*, 82.

²⁶ Denma Group, *The Art of War*, 70.

²⁷ Ibid., 71.

²⁸ Sawyer, *The Art of War*, 146.

Tao. If *Shih* can be conceived as an ever-changing state of strategic configuration as relative power and position evolve throughout the environment, *Tao* is the set of patterns we can observe that enable us to understand, predict and shape the changes evident in our environment. *Tao* is usually translated as “the way” and we can think of an object’s *Tao* as its fundamental nature. The *Tao* of water is to flow downhill. It is both what it is and how it acts. “The world, then, consists not of solid things but of flows of forces or movements of energy or shifting configurations of *Shih*. These are *Tao*.”²⁹ Literally described, *Tao* is, “... a roadway, or path, the way something works and equally a recommended course of action, the way it should be done,”³⁰ *Tao* describes how the various aspects in the environment work and allows us to anticipate events. “The intelligible pattern that can be discerned and mapped from each different perspective within the world is *Tao* – a ‘pathway’ that can, in varying degrees, be traced out to make one’s place and one’s context coherent.”³¹

The combination of *Shih* and *Tao* provides the foundation of strategy. If one understands the *Tao* of the strategic environment, not only can one comprehend the current configuration of *Shih*, one can also predict future states of *Shih* and with skill one can even shape or create *Shih*. “It may be simplest to take advantage of naturally occurring *Shih*, but it’s also wise to learn the small alterations you can make to the environment so that it works suddenly in your favor.”³² This, in essence, is Sun Tzu’s most basic formulation of strategy. “Having paid heed to the advantages of my plans, the general must create situations which will contribute to their

²⁹ Denma Group, *The Art of War*, 77.

³⁰ Ibid., 128.

³¹ Ames, *The Art of Warfare*, 50.

³² Denma, *The Art of War*, 77.

accomplishment. By ‘situations’ I mean he should act expediently in accordance with what is advantageous and so control the balance.”³³

Supporting Principles. Creating or exploiting naturally occurring *Shih* relies on several supporting principles that bear a remarkable similarity to our own Principles of War: initiative, knowledge, deception, surprise, flexibility and creativity. The first supporting principle is initiative. Strategy is competitive and exists in the minds of opposing commanders as each strives to shape the environment to match superior force with superior position. The resulting superior configuration of power enables a wise commander to force a decision by denying the enemy the space and time needed to adapt or react. As in chess, one does not necessarily have to destroy the enemy if one can effectively checkmate them by constraining or eliminating their ability to adapt or react and deny any options other than their destruction. In this context, Sun Tzu advises, “Therefore, the best military policy is to attack strategies ...”³⁴ The Denma Group notes, “The approach of taking whole first targets enemy strategy, undoing the coherence of the plan. The battle is won in the mind.”³⁵ Similarly, Ames refers to a commander’s wisdom as, “... a cognitive understanding of those circumstances that bear on the local situation, an awareness of possible futures, the deliberate selection of one of these futures, and the capacity to manipulate the prevailing circumstances and to dispose of them in such a way as to realize the desired future.”³⁶ Thus, Sun Tzu’s emphasis on initiative is apparent when he states, “Victory can be created. Even though the enemy has the strength of numbers, we can prevent him from

³³ Griffith, *The Art of War*, 66.

³⁴ Ames, *The Art of Warfare*, 111.

³⁵ Denma Group, *The Art of War*, 141.

³⁶ Ames, *The Art of Warfare*, 92.

fighting us.”³⁷ The active controlling aspect of strategy rests on the supporting principles of knowledge, deception and surprise.

Sun Tzu notes throughout *The Art of War* that possessing superior knowledge of the situation is imperative to creating and exploiting *Shih*. Knowledge comes from a disciplined analysis of all variables with primary emphasis on the opposing commander. “Absolute standards are unnecessary: the general seeks knowledge by contrasting various qualities, since strength and weakness, self and other, are relative. Thus he knows victory.”³⁸ The concept of “knowing victory” cannot be over-emphasized. It is in this context that Sun Tzu presents one of his most famous, if not always fully understood maxims, “He who knows the enemy and himself will never in a hundred battles be at risk...”³⁹ Knowledge and risk management are inseparable. “Knowledge protects one from danger. The general must know both self and other, conditions here and conditions there. This requires an ability to penetrate all aspects of the world.”⁴⁰

Denying adversaries information about the environment and oneself through deception or appearing formless is equally important. Hence, Sun Tzu famously said, “All warfare is based on deception.”⁴¹ But less well known is Sun Tzu’s argument for remaining unknown or “formless” even to one’s own forces. In a world where adversaries will employ spies of their own, constantly devising deceptive patterns and remaining formless or unknowable serve to constrain the enemy’s ability to assess the *Tao* of a given situation. “The ultimate skill in taking

³⁷ Ames, *The Art of Warfare*, 126.

³⁸ Ibid., 131.

³⁹ Ames, *The Art of Warfare*, 113.

⁴⁰ Denma Group, *The Art of War*, 145.

⁴¹ Griffith, *The Art of War*, 66.

up a strategic position (*hsing*) is to have no form (*hsing*). If your position is formless (*hsing*), the most carefully concealed spies will not be able to get a look at it, and the wisest counselors will not be able to lay plans against it.”⁴² Remaining formless and employing deception serve one purpose – to make the opposing commander misjudge the situation long enough to surprise them with superior power and position or *Shih*. Sawyer reinforces the link between deception and *Shih*.

Deceit is of course not practiced as an art or an end in itself, contrary to tendencies sometimes prevailing in the modern world ... such acts are all designed to further the single objective of deceiving the enemy so that he will be confused or forced to respond in a predetermined way and thereby provide the army with an exploitable advantage ... deception and manipulation are actually aspects of the greater question of form (*hsing*) and the formless.⁴³

Finally, surprise and deception depend on flexibility and creativity. If one provides an adversary enough time or space to adapt and react to a situation then the momentary advantage of *Shih* is lost. Flexibility and creativity are the principles that enable skilled commanders to combine superior power with superior position. “Victories depend on *Shih*, whose configuration is never constant. The general must recognize a momentary advantage, capturing victory as it arises.”⁴⁴ Sun Tzu employs the analogy of water adapting and matching its form to that of the terrain while it rushes down to the decisive point. “A central theme ... is the need for flexibility and negotiation in dealing with the specific conditions that make each situation particular. In the business of war, there is no invariable strategic advantage (*Shih*) which can be relied upon at all times.”⁴⁵

⁴² Ames, *The Art of Warfare*, 126.

⁴³ Sawyer, *The Art of War*, 136-137.

⁴⁴ Denma Group, *The Art of War*, 133.

⁴⁵ Ames, *The Art of Warfare*, 80.

ANALYSIS

The purpose of this section is to integrate the *Art of War's* concept of strategy with the characteristics of cyberspace. The model in Figure 1 uses an inside-out approach with the circle in the center representing the space-time available to an adversary. The circle should be viewed as dynamic - growing larger or smaller as freedom to adapt and react is augmented or diminished. Directly around the space-time circle and constraining it are the two attributes of *Shih* - superior force and superior position. *Tao*, as a key enabler joins the two attributes of *Shih* with the supporting principles of initiative, knowledge, deception, surprise, flexibility, and creativity depicted above. At the top are the core capabilities of cyberspace: attack, exploitation and defense which are achieved through a combination of physical and informational cyberspace effects.

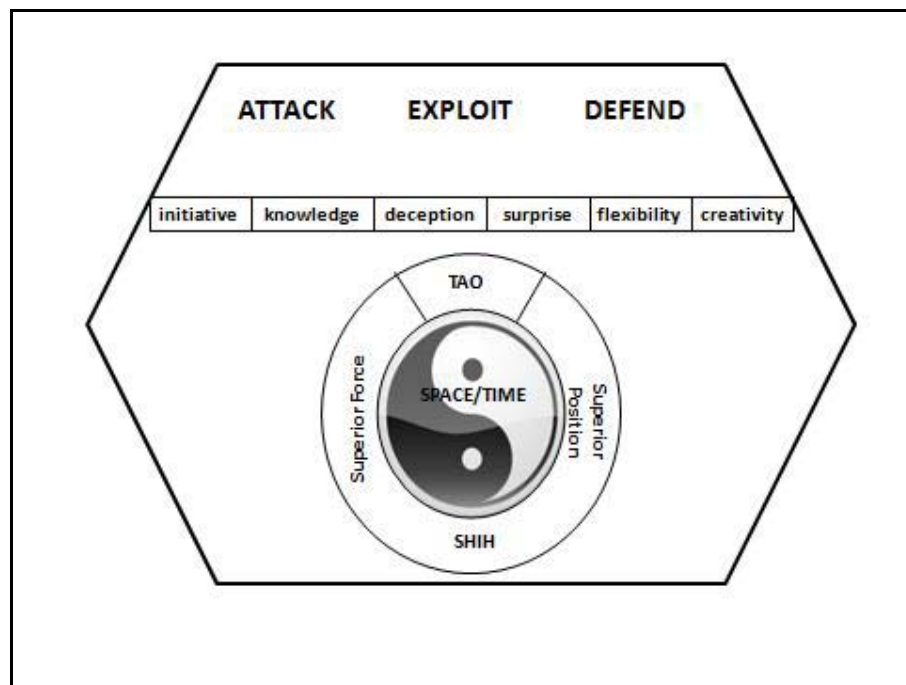


Figure 1. Cyberspace/Sun Tzu Strategy Model

Cyber Attack. The cyber attack section makes a three-part argument. First, the use of force in any domain tends to be most decisive at the tactical/operational level and least decisive at the strategic level. This has been evident throughout history and the experiences of the air domain provides a useful example. Cyberspace capabilities will not prove exceptional in this regard and the concepts and principles from *The Art of War* help explain this phenomenon. Second, the mix of available physical and informational cyber capabilities differs between the different levels of war. Strategic and non-state actor attack options will include physical and informational cyber capabilities while tactical/operational attack options will be limited to informational cyber capabilities. Combining the first two arguments leads to the third argument that cyber capabilities will most effectively contribute to strategy at the tactical/operational levels of war and will contribute less at the strategic level and to non-state actors.

Relative Decisiveness. All forms of combat with the exception of nuclear war have tended to be more decisive at the tactical/operational levels than at the strategic level of war.

Daniel Gouré frames this concept in terms of scale and scope.

At the strategic level, the reasons for continued difficulty in conducting decisive warfare came from the increasing scale and scope of combat. As military capability increased, so too did the territory over which wars were fought ... in a sense, the capability for destruction was constantly outpaced by increases in the demand for coverage.⁴⁶

⁴⁶ Gouré, *The Impact of the Information Revolution on Strategy and Doctrine*, 222.

Additionally, Clausewitz notes the importance of the freedom to adapt and react that usually remains available to strategic decision makers even after significant losses. “A government must never assume that its country’s fate, its whole existence, hangs on the outcome of a single battle, no matter how decisive. Even after a defeat, there is always the possibility that a turn of fortune can be brought about by developing new sources of internal strength ...”⁴⁷

This leads to the example of early air power theorists such as Douhet. While studying a new technology with apparently unrestricted strategic access, Douhet predicted strategic airpower attacks would prove decisive if targeted against civilian populations. However, his prediction wasn’t realized during “strategic” bombing campaigns. Overy notes, “The naive expectation that bombing would somehow produce a tidal wave of panic and disillusionment which would wash away popular support for war and topple governments built on sand was exposed as wishful thinking.”⁴⁸ Robert Pape’s excellent study on coercion provides a similar argument, “...strategic air power cannot be decisive. The most it can do is to reduce the costs that friendly land and theater [tactical/operational] air forces have to pay to defeat enemy forces on the battlefield.”⁴⁹ Like Clausewitz, Pape’s analysis reveals that decisiveness is essentially a function of the space-time available to decision makers to adapt and react. “Theater air power is a much stronger coercive tool ...it gives the opponent much less scope to minimize consequences because effects are more immediate.”⁵⁰

⁴⁷ Clausewitz, *On War*, 483.

⁴⁸ Overy, *Why the Allies Won*, 132.

⁴⁹ Pape, *Bombing to Win*, 317.

⁵⁰ *Ibid.*, 318.

Although he doesn't use the term, Pape is describing *Shih* and he even uses a Sun Tzu-like analogy of a hammer and anvil to describe the decisiveness of theater-level airpower.⁵¹ The model in Figure 1 helps to explain this. If the objective of strategy is to constrain an adversary's space-time, deny their freedom to adapt and react and force a decision then it's reasonable to assume decisiveness is more easily achieved at the tactical/operational levels where space-time is already the smallest and freedom to adapt and react is more naturally constrained. Likewise, decisiveness is harder to achieve at the strategic level where the space-time available to decision makers is already the largest and freedom to adapt and react is less naturally constrained despite the employment of significant physical force.

Capabilities Mix. The mix of physical and informational cyber capabilities differs between the various levels of war. Strategic and non-state actor attack options include physical and informational cyber capabilities while tactical/operational attack options are limited to informational cyber capabilities. The next section analyzes this observation, along with the relative decisiveness of cyber capabilities from the perspectives of strategic, tactical/operational and non-state actors.

Strategic Level. Theories predicting a decisive cyberspace role focus on modern society's reliance on networked systems and the potential enormity of the physical effects that can be directed towards civilian populations through cyberspace. "... the battleground is the information infrastructure upon which modern societies have become so dependent, including the electrical power grid, the financial system, the air traffic system, and a variety of sensitive

⁵¹ Ibid., 318.

computer systems.”⁵² These predictions along with predictions that strategic cyber attacks will induce overwhelming fear, panic and capitulation in civilian populations are similar to those of early airpower theorists. “This aspect of ‘information warfare’ has the side benefit for the attacker to create confusion, panic, and irrationality among the civilian target population further contributing to the weakening of its political ‘will-to-fight’ [and] information warfare aimed at the civilian information infrastructure may be the next major innovation in the domain of strategic warfare ...”⁵³

One could argue these predictions focus on the ability to generate significant cyberspace effects without fully considering whether the effects contribute to strategy. Some theorists are beginning to argue against the decisiveness of strategic cyber attacks using logic that’s closely linked to Sun Tzu’s emphasis on space-time, or *Shih*. Martin Libicki makes this argument by comparing the time-space consequences of strategic cyber attacks to those of a snowstorm. “There is a big difference between disabling a system temporarily and doing so for a great length of time. ... even a successful widespread information attack has more the character of a snowstorm ... it is not that they’re smaller [than nuclear firestorms] ... but the effect is entirely temporary and rapidly over.”⁵⁴ David Lonsdale reinforces the argument with a strategic bombing analogy saying, “The notion that a population, or state, would surrender as a result of

⁵² Shapiro, *Information and War: Is it a Revolution?*, 131.

⁵³ Rona, *Scorched Earth to Information Warfare*, 10-11.

⁵⁴ Libicki, *Conquest in Cyberspace*, 37 - 39.

its electricity or banking system going down in the face of SIW [strategic information warfare] is difficult to accept in the light of the experience of strategic bombing.”⁵⁵

War is a human endeavor and people resist capitulation as long as there is sufficient space-time available to continue resisting. Strategic cyber attack options include potentially significant and disruptive informational and physical capabilities but their power can't be matched with the superior position required to create *Shih*. Whether the domain is cyberspace or the air, “There are two serious shortcomings with distant [strategic] punishment; first, firepower alone is seldom determinant (regardless of the volume, lethality, or precision); and second, over-reliance ignores the psychology of the opponent's will to resist ... the ‘losers’ rightly do not understand they lost.”⁵⁶

Tactical/Operational. Tactical/operational level cyber attack capabilities will take the form of information rather than physical effects. Information itself has not been weaponized and can't provide superior force but it exists as a key enabler for achieving superior position through deception and surprise. “Cyber capabilities can assuredly support the application of other force capabilities, but fundamentally, they are not the destructive, kinetic, purveyors of violence that war fighters traditionally envision in planning military strategies, engagements, and war.”⁵⁷

Some have argued tactical/operational level information will be so important to warfare that control of information alone will become the decisive factor rather than the physical destruction of adversary forces. Arquilla and Ronfeldt, argue, “... decisive duals for the control

⁵⁵ Lonsdale, *The Nature of War in the Information Age*, 166.

⁵⁶ Dearth, *The Human Factor in Future Conflict: Continuity and Change*, 14.

⁵⁷ Convertino, DeMattei and Knierim, *Flying and Fighting in Cyberspace*, 14.

of information flows will take the place of drawn-out battles of attrition or annihilation; the requirement to destroy will recede as the ability to disrupt is enhanced.”⁵⁸ Additionally, Andrew Marshall argues,

... protecting the effective and continuous operation of one’s own information systems and being able to degrade, destroy, or disrupt the functioning of the opponent’s information systems will become a major focus of the operational art ... it has always been important. It will soon be central.⁵⁹

These arguments are less persuasive when viewed through Figure 1. A cyberspace attack may temporarily blind, disorient or confuse an adversary at the tactical/operational level but surprise isn’t decisive unless it matches superior force with superior position and eliminates the space/time needed to adapt and react. It’s not coincidental that the tactical/operational level of today’s warfare most closely resembles the conditions that existed at the time of Sun Tzu’s writings. The *Art of War* places great emphasis on deception and surprise in part because they’re inherently easier to achieve in constrained space-time. This is why Handel argues Sun Tzu and Clausewitz provide apparently conflicting perspectives on the value of surprise. “... when Clausewitz speaks of the near-impossibility of achieving surprise, he is primarily referring to the higher operational or strategic levels, whereas Sun Tzu’s high estimation of the utility of surprise is mainly in the context of tactical level.”⁶⁰

Non-state actors. Non-state actors such as terrorists may prove more constrained in their use of cyber attack options than many assume. Some have argued cyber attacks are custom-

⁵⁸ Arquilla and Ronfeldt, *A New Epoch – And Spectrum – Of Conflict*, 2.

⁵⁹ Marshall, *Forward to Strategic Appraisal: The Changing Role of Information in Warfare*, 5.

⁶⁰ Handel, *Masters of War*, 227.

made for terrorism due to their inherent anonymity and the potential for significant strategic effects. However, in an age when terrorists have demonstrated the will to kill thousands through traditional kinetic means cyber terror attacks still haven't occurred. Gabriel Weimann argues, "... cyber terrorism now ranks alongside other weapons of mass destruction in the public consciousness ... but there's just one problem: there is no such thing as cyber terrorism – no instance of anyone ever having been killed by a terrorist (or anyone else) by a computer."⁶¹ Maura Conway similarly notes, "The problem [of cyber terrorism] certainly can't shrink much, hovering as it does at zero cyber terrorism incidents a year."⁶²

The Art of War may help explain this through the familiar space-time argument. As its name suggests, terrorism's effectiveness is based on the ability to create terror. Causing inconvenience or major disruption is not the same as unleashing random violence and killing civilians. Weimann argues that for a cyber terrorism attack to, "... intimidate or coerce a government or its people in furtherance of political or social objectives ... an attack should result in violence against persons or property, or at least cause enough harm to generate fear."⁶³ It's possible that terrorists share the same strategic-level weakness as state actors. While terrorists can potentially generate strategic-level effects, the effects will fail to produce the immediateness needed to generate fear and contribute to terrorists' strategies. Ironically, terrorists may also share tactical/operational-level weaknesses because tactical cyber capabilities aren't weaponized and can't contribute violent acts. "Traditional terrorism generally involves violence or threats of

⁶¹ Weimann, *Terror on the Internet*, 149.

⁶² Conway, *Cyberterrorism: Hype and Reality*, 93.

⁶³ *Ibid.*, 153.

violence. However ... ‘cyber violence’ is still very much an undefined activity.”⁶⁴ The tactical/operational information capabilities that contribute to surprise in traditional war provide little advantage to terrorists who target unsuspecting civilians and don’t need to “generate” surprise. *Shih* tends to exist naturally for terrorists because they target non-combatants who are unaware of the engagement.

While the jury is still out on cyber terrorism, a case can be made that cyber terrorist attacks remain difficult to execute and may be perceived by terrorists as ineffective in contributing to strategy. “For the foreseeable future, cyber terrorism [attacks]... will be very difficult to perform, unreliable in their impact, and easy to respond to in relatively short periods of time.”⁶⁵

Cyber Attack Effectiveness. Combining the relative mix of strategic, tactical/operational and non-state actor capabilities with their potential decisiveness leads to the counter-intuitive conclusion that strategic physical/informational cyber attacks and terrorist cyber attacks will prove ineffective and will contribute less to strategy than tactical/operational-level informational capabilities. This does not mean the often predicted cyber “Pearl Harbor” won’t occur. Like airpower, cyber attack provides a means of inflicting distant punishment whose, “... ease of use and apparent low risk make it deceptively attractive ...”⁶⁶ Perhaps, the best way to view a potential cyber Pearl Harbor is by considering the real one. The Japanese achieved strategic surprise and a tactical/operational victory but the effects weren’t decisive enough to prevent an American response that ultimately proved disastrous for Japan. In arguing against the surprise

⁶⁴ Ibid., 80.

⁶⁵ Weimann, *Terror on the Internet*, 148.

⁶⁶ Dearth, *The Human Factor in Future Conflict: Continuity and Change*, 14.

attack, the Japanese Naval Chief of Staff tellingly observed the importance of space, time, power and position to strategy. “Even if our Empire should win a decisive naval victory ... we will not thereby be able to bring the war to a conclusion. We can anticipate that America will attempt to prolong the war, utilizing her impregnable position, her superior industrial power, and her abundant resources.”⁶⁷

Cyber Exploitation. Cyber exploitation is a joint term describing cyber intelligence, surveillance and reconnaissance (ISR) and is the cyber equivalent of intelligence preparation of the operational environment (IPOE).⁶⁸ Exploiting the information that exists in adversarial cyberspace is important for several reasons. First, Sun Tzu repeatedly emphasizes that knowledge is critical to creating or exploiting *Shih* and hence, knowledge is the prerequisite of victory. Second, in contrast to cyber attack options, cyber exploit options will prove valuable at all levels of war. Third, cyberspace is man-made and dynamic. Hostile cyber activities require a thorough knowledge of an adversary’s changing cyberspace architecture. Consequently, knowledge of cyberspace itself has become a new and critical collection requirement in its own right. Fourth, Sun Tzu advocates for initiative in intelligence gathering and cautions against combat when possible. Exploitation may prove to be the primary form of hostile cyber activity between current and rising great nations while armed combat is limited to the periphery to lower risk and costs.

⁶⁷ Iklé, *Every War Must End*, 3.

⁶⁸ Convertino, DeMattei and Knierim, *Flying and Fighting in Cyberspace*, 44.

Contribution to *Shih*. Much of the information needed to exploit or create *Shih* exists in cyberspace and is vulnerable to exploitation. Sun Tzu repeatedly emphasizes that knowledge is critical to the ability to limit risks and exploit or create *Shih*. Knowledge in itself is not the object. Knowledge is needed to fully understand all variables and know when, where and how to exploit or create *Shih*. The Denma Group makes this point saying, “Because you have taken the measure of things, you know their true weight. Victory is then arranging the balance to create preponderance. Like the release of water down a steep ravine, this is *Shih*.”⁶⁹ According to Convertino, DeMattei and Knierim, “Cyberspace directly enables the information-based war envisioned in Sun Tzu’s theories, immediately capturing the concept of achieving information advantage and applying it to execute and win wars.”⁷⁰

Levels of War. Cyber exploitation is also important because it provides valuable information at all levels of war. In contrast to cyber attacks that contribute to strategy primarily at the tactical/operational level, the exploitation of intelligence has no similar boundaries. In fact strategic information, if successfully exfiltrated is of paramount importance. “Foresight in diplomatic affairs can be a crucial advantage ... the ability to know what the adversary will propose and what his goals are is a strategic advantage that cannot be ignored.”⁷¹

Collection Means and Subject. The third reason cyber exploitation is important is that cyberspace is man-made and dynamic. In one sense, gathering information in cyberspace can be simply characterized as a new tool for accomplishing one of the oldest known professions –

⁶⁹ Denma Group, *The Art of War*, 150.

⁷⁰ Convertino, DeMattei and Knierim, *Flying and Fighting in Cyberspace*, 36.

⁷¹ *Ibid.*, 58.

spying. As Timothy Thomas asked, “Exploiting information about the number and location of enemy forces, as well as the composition of his own force, was key to the decision-making of Genghis-Khan. Does ‘information age’ really define anything new?”⁷² However the cyber domain has brought an important change. One of the challenges of cyber exploitation lies in understanding the architecture of the adversary’s cyberspace systems to ensure they can be infiltrated and/or attacked when needed. This is challenging because a wide variety of deliberate and incidental activities can dramatically alter the cyber landscape over time. Systems are routinely modified, upgraded or abandoned and information is deleted, archived or moved.

Not only is considerable effort, often spanning several months or years, required to scope adversary systems, but the efforts must be constantly renewed in order to validate their relevance at the time of attack. And even then, the descent into crisis and war is often the moment that they change the most, as users suddenly begin to take their security much more seriously.⁷³

In essence, cyberspace provides both a new medium and a compelling new subject for exploitation – the destination and the path. This new requirement to “know” potential adversarial systems is so compelling that cyber exploitation will be systematically accomplished against friend and foe well before attacks are considered. Martin Libicki notes, “...intelligence preparation of the battlefield – a must – requires hacking prior to having the information that would justify permission to do so.”⁷⁴

National Security Role. Finally, cyber exploitation requires initiative and will assume a central if not defining role in national security. “The unvarying rule is never to rely upon the

⁷² Thomas, *Cyber Silhouettes*, 12.

⁷³ Thomas, *Cyber Silhouettes*, 99.

⁷⁴ Libicki, *Conquest in Cyberspace*, 257.

good will of others, not upon fortuitous circumstances, but guarantee – through knowledge, persistent analysis, and defensive preparation – that the enemy can neither mount a surprise attack nor gain a victory through simple coercion.”⁷⁵ Thus, an additional constraint on a cyberspace Pearl Harbor is that it could reveal the attacker’s capabilities, tactics, techniques and procedures and bolster the target nation’s defenses. “One places a greater premium on stealth and low probability of detection than one does in many kinetic operations because activities in the cyber domain depend upon continued access to target systems; detection could result in loss of access due to disconnection or improved security.”⁷⁶

Perhaps the US-Soviet Cold War provides a model of future great power cyber hostilities with the familiar spy/counter spy dynamic at once both defining and moderating the conflict’s nature. “This type of warfare straddles the continuum of political, strategic, operational, and tactical levels of war. It is waged continuously at all levels, through peacetime, crisis, escalation, conflict, war, war termination, and restoration. It is the art of survival.”⁷⁷ It is possible that many hostile cyber actions will be difficult to characterize as either an attack or an exploit. Future combatants may initiate disruptive and even destructive cyber operations with the intent of proving attack concepts and capabilities. It will be difficult to know if an attack was just an attack or if it was a means of assessing an adversary’s capabilities, reactions and vulnerabilities. In this regard, cyber attack and exploit will be a murky ground as nations probe and assess each other’s cyberspace architecture. “Intelligence is cousin to deception. As hiding and seeking

⁷⁵ Sawyer, *The Art of War*, 135.

⁷⁶ Convertino, DeMattei and Knierim, *Flying and Fighting in Cyberspace*, 43.

⁷⁷ Nelson, *The Art of Information War*, x.

assume larger roles in outcomes, each side will necessarily put more effort into testing each other's capabilities, to see what is and is not detectable.”⁷⁸

CYBER DEFENSE

This section begins by arguing cyberspace is in its infancy, defenders will adapt to cyber threat capabilities and many of the advantages currently inherent in cyber attack will be mitigated with time. Next, it analyses how cyber defense contributes to strategy through Sun Tzu's metaphor of formlessness and two concepts: security and unpredictability. Then it presents potential tactics, techniques and procedures that may prove valuable in bolstering cyber defenses based on combining both models in a mutually supportive manner.

Defensive Adaptation. Cyberspace, as a warfighting domain, is in its infancy. As impressive as current technologies are they will almost certainly appear as unsophisticated as the Wright Brothers' aircraft appeared just a few decades after the first flight. This is important because one of cyberspace's "truisms" is that it is inherently difficult to defend. The Air Force Research Lab (AFRL) notes that, "Many describe cyberspace as a domain that favors the attacker ... Defensive operations are constantly playing "catch up" to an ever-increasing onslaught of attacks that seem to always stay one step ahead.”⁷⁹ Interestingly, another of the predictions that Douhet got wrong regarding the development of airpower was the inherent strength of the offense. In language that is strikingly similar to AFRL's he predicted,

⁷⁸ Libicki, *Defending Cyberspace and Other Metaphors*, 70.

⁷⁹ AFRL, *Integrated Cyber Defense and Support Technologies*.

The greatest advantage of the offensive is having the initiative in planning operations – that is, being free to choose the point of attack and able to shift its maximum striking forces; whereas the enemy, on the defensive and not knowing the direction of the attack, is compelled to spread his forces thinly to cover all possible points of attack ... in that fact lies essentially the whole game of war tactics and strategy.⁸⁰

What Douhet could not predict were the defensive technological advances and elaborate integrated air defense systems that would emerge as nations adapted to airpower threats. Similarly, the rest of this section rests on the assumption that offensive cyber attackers currently possess clear advantages but that effective defensive capabilities will emerge and they will rely on technological advances. “The history of war-fighting in this century has been one in which technological changes have played a major role in the outcome and the ability of nations to defend themselves effectively has, in large measure, depended on access to technology at least equal to that of the adversary.”⁸¹

Two-Model Defense. *The Art of War* provides guidance for the development of these technologies and capabilities by emphasizing formlessness. “The ultimate in disposing one’s troops is to be without ascertainable shape. Then the most penetrating spies cannot pry in nor can the wise lay plans against you.”⁸² Michael Handel argues this leads to a defensive strategy based on two models. “In the process of gathering the best possible intelligence on his enemy, a successful leader must also prevent his enemy from doing likewise. This can be accomplished

⁸⁰ Douhet, *Command of the Air*, 15-16.

⁸¹ Schwartzstein, *Introduction to The Information Revolution and National Security*, xvii.

⁸² Griffith, *The Art of War*, 100.

through two main methods: security and unpredictability.”⁸³ The security model is focused on protecting access to information and has been the traditional framework for cyber defense.

“Traditionally our information systems are seen as fortresses that must be fortified against attack – but the advantage remains with the attacker”⁸⁴ Several theorists argue the security model fails in cyberspace because cyberspace is comprised of networks and networks are designed to let others in and share information. The dilemma is providing access to authorized users while keeping adversaries out. As Robert Ghanea-Hercock points out, “There is no inside or outside [in cyberspace], only a continuous spectrum of risk and trust”⁸⁵ The unpredictability model makes friendly cyberspace difficult for adversaries to know and understand through two concepts: formlessness and deception. The strategy of using technology to remain formless and deceptive differs from most approaches to cyber defense which focus on providing security, but as Ralph Sawyers notes, “By integrating these two principles, a foe can be manipulated and vital secrecy preserved.”⁸⁶ The next two sections review potential tactics, techniques and procedures that can be developed and employed in support of the security and unpredictability models.

Security Model. Convertino, DeMattei and Knierim provide a good framework for the traditional security model in the Air University Maxwell Paper, *Flying and Fighting in Cyberspace* by breaking cyber security into five categories: a) Protection from Attack, b) Attack

⁸³ Handel, *Masters of War*, 235.

⁸⁴ Rowe and Rothstein, *Deception for Defense of Information Systems*.

⁸⁵ Ghanea-Hercock, *The Art of Cyberwar*, SecurityPark.net.

⁸⁶ Sawyer, *The Art of War*, 138.

Detection and Attribution, c) Automated Attack Response and Operator Alert, d) Self-healing Networks and Systems, and e) Rapid Recovery.⁸⁷

Protection from attack includes many traditional technologies such as firewalls, access control measures and patching known vulnerabilities. Noting that these techniques are inherently reactive, some have argued security should be built into cyberspace by revising its basic rule sets. For example, AFRL argues,

... since cyberspace is a man-made technological domain, the "laws" of cyberspace can be re-written, and therefore the domain can be modified at any level to favor defensive forces. We need to modify, extend, or replace vulnerable and insufficient protocols, architectures, instruction sets, etc. as necessary to secure critical warfighting systems.⁸⁸

Rick Wesson, CEO of Support Intelligence, counters that these important changes will prove problematic because of their global impact. Noting that cyberspace was originally designed by DOD agencies well before security was an issue he ironically notes, "Even a founding father can't unilaterally change things that the entirety of the internet ecosystem now depends on."⁸⁹ The second security category includes IP trace back, geo-location, and determination of intent.⁹⁰ These techniques counter the anonymity that provides much of the advantage to cyber attackers and reduce the ambiguity of an intruder's intent. "Responding to

⁸⁷ Convertino, DeMattei and Knierim, *Flying and Fighting in Cyberspace*, 52-54.

⁸⁸ AFRL, *Integrated Cyber Defense and Support Technologies*.

⁸⁹ Rick Wesson, *Air Force Aims to 'Rewrite Laws of Cyberspace'*.

⁹⁰ AFRL, *Integrated Cyber Defense and Support Technologies*.

someone's destructive electronic intent in an imprecise science ... it is very difficult to ensure that the culprit in question was actually the one who initiated the action.”⁹¹

While the first two security categories were focused on preventing attacks, the next three security categories are focused on mitigating the consequences of an attack, improving attack responses and continuing operations. Automated attack response techniques are designed to ensure defensive operations can respond at the same tempo as attack options. Some have argued game theory could provide a means of developing a set of response “playbooks” that could anticipate an attacker's likely actions and provide automatic and timely responses to the attack.⁹² Self regenerative code allows attacked organizations, “... to fight through cyber attacks by enabling information systems to learn, regenerate themselves in response to unforeseen errors and/or attacks, and automatically improve their ability to deliver critical services.”⁹³ Self regenerative networks employ graceful degradation techniques to ensure systems can continue to provide a basic level of service during attacks, rapidly reconstitute system parameters and data and provide persistence. Finally, rapid recovery from attack techniques exploit advancements in memory to ensure even complex systems could recover from disruption or even destruction in minutes and at relatively low cost.

Unpredictability Model. The unpredictability model has two main components – formlessness and deception. Formlessness contributes to strategy by making friendly cyberspace

⁹¹ Thomas, *Cyber Silhouettes*, 205.

⁹² Tinnel, Saydjari and Farrell, *Cyber Strategy and Tactics*.

⁹³ AFRL, *Integrated Cyber Defense and Support Technologies*.

architectures difficult to understand and exploit. Deception applies to the design of cyberspace architectures and to the data that resides in them.

Formlessness techniques include encryption, polymorphic networking, rapidly reconfigurable system parameters and dynamic protocols. Encryption transforms information using an algorithm or cipher to make it unreadable to anyone who doesn't have the key. Skilled and persistent adversaries can break most current encryption methods but this takes time. Thus, encryption technologies are most effective when used to augment other techniques because encryption complicates an intruder's task. Polymorphic computer code is similar to encryption, but instead of changing the nature of data it changes or mutates cyberspace architectures. Interestingly, these techniques are already being used in computer viruses to avoid pattern recognition algorithms in virus scanning software.⁹⁴ "Everything Hopping" is an AFRL term that describes dynamic networking systems in which all components would simultaneously and rapidly reconfigure parameters in a manner similar to the frequency hopping that occurs on secure radios today.⁹⁵ Although these techniques differ in their approach, the common objective is to make friendly cyberspace difficult to understand if security is compromised. The AFRL is researching many of these techniques and explains the concept this way.

Avoiding threats in real-time is accomplished through the use of polymorphic techniques to present an agile "moving target" that allows systems to employ evasion tactics, and escape tactics if a viable threat is confronted. The ability to modify the domain will be leveraged so that modification can take place many

⁹⁴ AFRL, *Integrated Cyber Defense and Support Technologies*.

⁹⁵ Ibid.

times per second at multiple layers of networking. Thus, the attacker loses the advantage of time and the benefit of previously collected intelligence.⁹⁶

As Roger Ames notes, “Another way to achieve this desired ‘formlessness’ is through deceit”⁹⁷ and the first deceptive technique focuses on cyberspace architectures. Honeypots are an existing and relatively simple example of a deceptive technique. Honeypots are,

“... a resource that has no authorized activity, they do not have any production value. Theoretically, a honeypot should see no traffic because it has no legitimate activity. This means any interaction with a honeypot is most likely unauthorized or malicious activity. Any connection attempts to a honeypot are most likely a probe, attack, or compromise.”⁹⁸

The purpose, says Lance Spitzner, is deception. “The idea is to confuse an attacker, to make him waste his time and resources interacting with honeypots.”⁹⁹ Michael, Auguston and Rowe recommend expanding honeypots with a concept they call intelligent software decoys.¹⁰⁰ Software decoys would be more active than current honeypots and would be designed to tolerate intrusions, learn from attack methods and then neutralize attacks. The objective is to deceive the intruder into terminating the attack without revealing your intentions by either creating believable friction to reduce the intruder’s will, changing the proximity of the attack to a

⁹⁶ AFRL, *Integrated Cyber Defense and Support Technologies*.

⁹⁷ Ames, *The Art of Warfare*, 95.

⁹⁸ Spitzner, *Honeypots: Definitions and Value*

⁹⁹ Ibid.

¹⁰⁰ Michael, Auguston and Rowe, *Software Decoys: Intrusion and Detection and Countermeasures*.

honeypot or if other options fail by eliminating the intruder's capabilities by closing ports or killing processes.¹⁰¹

Deceptive cyberspace defense techniques can also be applied to the information that exists in cyberspace. Using language that is reminiscent of Sun Tzu, Rowe and Rothstein argue these methods share four basic objectives: a) to increase friendly freedom of action by diverting the adversary's attention from the real action, b) to persuade an adversary to adopt courses of action that are to their disadvantage, c) to gain surprise and d) to preserve friendly resources and reduce risk.¹⁰² In a comparison between deception in cyberspace and conventional warfare, they recommend four defensive techniques including: a) concealment of important settings and files, b) planting lies such as false error messages, c) presenting displays so intruders "see" expected attack effects such as system slowdowns and d) employing feints to distract intruder away from critical areas.¹⁰³

The specific security and unpredictability techniques presented here may or may not prove viable, but they provide insight into the potential for improving cyber defense by expanding the traditional concept of security and incorporating *The Art Of War's* emphasis on unpredictability through formlessness and deception. The unpredictability model also supports the security model by providing useful intelligence on adversarial capabilities and intentions. The Denma Group makes this point regarding Sun Tzu and the benefits of appearing formless or unknowable. "Your form cannot be assessed by spies or strategists because there is nothing

¹⁰¹ Ibid.

¹⁰² Rowe and Rothstein, *Deception for Defense of Information Systems: Analogies from Conventional Warfare*.

¹⁰³ Ibid.

there for them to grasp. Thus, they are formed by their own projections, which is all they can discern. These projections, in turn, reveal their position to you. This is the *Tao* of deception.”¹⁰⁴

CONCLUSIONS

This paper applied concepts from *The Art of War* to the three core cyberspace capabilities to answer how cyberspace can be expected to contribute to strategy. Applying Sun Tzu to the emerging cyberspace domain has merit because of *The Art of War*'s conceptual nature, timeless quality and its focus on strategy. Warfare remains a uniquely human endeavor regardless of the means employed. Although we are still discovering and writing the laws of cyberspace, Sun Tzu remains popular because the laws of strategy, or *Shih*, remain constant and relevant. According John Rothrock, “The best technology, even when employed with the greatest of tactical effectiveness, can be counterproductive if the technology and its employment are not orchestrated against a set of well-conceived, hierarchically consistent operational, strategic, and policy objectives.”¹⁰⁵ Sun Tzu helps us understand the ultimate strategic purpose of operating in cyberspace which in turn leads to clarity in determining objectives.

The primary conclusion is that all three core cyberspace capabilities; attack, exploitation and defense will make critical contributions to strategy but in ways that are somewhat surprising

¹⁰⁴ Denma Group, *The Art of War*, 163.

¹⁰⁵ Rothrock, *In Athena's Camp*, 222.

and that conflict with some cyberspace predictions. The specific conclusions for each capability are presented next and are followed by some general conclusions and remarks.

Cyber Attack. Tactical/operational level information capabilities will enable forces to achieve superior position through deception and surprise and will achieve a significant role in strategy. Taken alone, strategic cyber attack options such as disrupting adversarial power grids will probably not be effective contributors to strategy. Even significantly disruptive and destructive strategic-level cyber effects will be general in nature and will lack the superior position needed to contribute to strategy. However, those identical capabilities will be very effective if they are made operational by integrating them into tactical/operational-level planning and force employment. Although state actors may be tempted by the possibility of distant punishment, strategic cyber attacks should be avoided in most situations because they'll be significant enough to demand a range of responses (possibly kinetic) from targeted nations without being decisive enough to prevent the responses and their consequences. In most cases such attacks would conflict with Sun Tzu's emphasis on taking whole because they increase the attacker's risks and costs while contributing little to strategy. According to Jon Jurich,

Some consensus exists that the world's major powers are unlikely to engage in offensive direct conflicts with each other by either traditional means or IW [information warfare]. In a world with established military and economic disparities, however, emerging nations and non-state actors that make traditional attempts to harm a dominant adversary will likely compete asymmetrically, making the use of IW more attractive to less well-heeled combatants.¹⁰⁶

¹⁰⁶ Jurich, *Cyberwar and Customary International Law*

Hence, terrorist cyber attack options are the most difficult to predict. Terrorists and non-state actors have many good reasons to find cyber attack options attractive but there are no documented instances of cyber terrorism yet. According to traditional definitions, terrorism requires a level of violence sufficient to induce terror in the public. Currently, no tactical/operational or strategic level cyber attack options enable terrorists to employ sufficiently focused violence to meet that definition.

Cyber Exploitation. Cyber exploitation is a reality and will continue to exist as a significant contributor to strategy. *The Art of War* is founded on the belief that commanders must “know” victory through knowledge. Cyberspace will provide a new means for obtaining information and will also provide a new subject to be studied because knowledge of adversarial cyberspace architectures is a prerequisite for initiating exploitation and/or attack options. Exploitation of adversarial information is so fundamental to strategy it will probably be the predominant form of hostile cyber activity in the foreseeable future. With that said, the line between cyber attack and cyber exploitation will be ambiguous. It’s difficult for targeted actors to know a cyber intruder’s intentions. Stealth will be a dominant factor but some attacks could actually be intended to force defenders to reveal capabilities, tactics, techniques and procedures. Whether disruptive or destructive intrusions are intended as attacks or exploits, the consequences for the targeted nation will be serious and a clear threat to strategy and national security.

Cyber Defense. Cyber defense will prove critical to national security and will be an important contributor to strategy. Cyber attackers currently possess significant advantages over cyber defenders but technological advances can be expected to mitigate these advantages. Sun Tzu’s strategy concepts from *The Art of War* make a compelling argument for broadening the traditional security-based defensive model through the adoption of a defensive strategy

comprised of security and unpredictability models. The security model looks inward. Its objective is to preserve the utility of friendly cyberspace during and after an attack by preventing attacks, mitigating attack consequences, improving attack responses and continuing friendly operations. The unpredictability model looks outward. Its objective is to deny intruders the utility derived from successful exploitation and to keep friendly intentions and strategies “unpredictable.” The unpredictability model benefits from formlessness and deception and makes friendly cyberspace difficult to understand or “formless” even if security is compromised. Many of the unpredictability model’s techniques allow defenders to observe and learn intruder tactics, techniques and procedures and directly support the security model. Both models will require significant technological advances to be effective and organizations like the Air Force Research Laboratory are researching many of these techniques today.

This paper’s focus on strategy simplified the task at hand, but failed to address some of the ambiguity that exists with regard to cyberspace. This leaves several interesting research questions unanswered. First, how can we expect cyber forces to be integrated with other force providers and how central of a role will cyber capabilities provide? If air power’s experience is a guide we can expect flexibility and creativity to dominate the employment of cyberspace capabilities. Cyber capabilities can be expected to provide combat support to other forces but they could also just as reasonably be the primary or even the exclusive force provider. It will all depend on context and strategy – or *Tao* and *Shih*.

Second, this paper focused on attack options with clear tactical/operational effects or strategic physical effects like taking down a power grid. But what, exactly, constitutes an attack? What distinguishes criminal activity from cyber attacks? Is that a false distinction? Is a new realm of political conflict emerging in the cyberspace domain in which a variety of actors can

conduct disruptive actions that are the cyber equivalent of political protests or riots? Would these actions qualify as warfare or even attacks if protests and riots don't?

Finally, Sun Tzu's concepts on strategy have been reinterpreted and applied in many contexts from sports to politics and business. If there is merit in studying *The Art of War* in these contexts what can Sun Tzu teach if there regarding cyberspace conflict that may not qualify as war? Given that Sun Tzu wrote during a time of political turmoil involving a variety of strong and weak warring states it seems *The Art of War's* timeless and conceptual nature may still be quite applicable. As Ames notes, "It [*Shih*] begins with a recognition that the business of war does not occur as some independent and isolated event, but unfolds within a broad field of unique natural, social, and political conditions."¹⁰⁷

¹⁰⁷ Ames, *The Art of War*, 76.

BIBLIOGRAPHY

Adams, James. *The Next World War*. New York, NY: Simon & Schuster, 1998.

Air Force Research Laboratory (AFRL) – Rome Research Site. *Integrated Cyber Defense and Support Technologies*, Solicitation Number: BAA-08-08-RIKA. Posted 14 Oct 08.
https://www.fbo.gov/index?s=opportunity&mode=form&id=e72854d6e3c1a044038563ef1e0fdfa6&tab=core&_cview=0&cck=1&au=&ck=.

Alberts, David S. *Defensive Information Warfare*. Washington DC: National Defense University, 1996.

Allard, C. Kenneth. “Information Warfare: The Burden of History and the Risk of Hubris.” In *The Information Revolution and National Security*. Washington DC: The Center for Strategic & International Studies, 1996.

Ames, Roger. *Sun-Tzu – The Art of Warfare*. New York, NY: Ballantine Books, 1993.

Anderson, Robert H., and Anthony C. Hearn. “An Exploration of Cyberspace Security R&D Investment Strategies for DARPA. In *In Athena’s Camp*. Edited by John Arquilla and David Ronfeldt. Santa Monica, CA: Rand, 1997.

Arquilla John and David Ronfeldt. “A New Epoch – And Spectrum – Of Conflict” In *In Athena’s Camp*. Edited by John Arquilla and David Ronfeldt. Santa Monica, CA: Rand, 1997.

Arquilla John and David Ronfeldt. “Information. Power, and Grand Strategy: In *In Athena’s Camp*. Edited by John Arquilla and David Ronfeldt. Santa Monica, CA: Rand, 1997.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Cooper, Jeffrey R. “Another View of Information Warfare: Conflict in the Information Age.” In *The Information Revolution and National Security*. Washington DC: The Center for Strategic & International Studies, 1996.

Convertino II, Sebastian M., Lou Anne DeMattei, and Tammy M. Knierim. *Flying and Fighting in Cyberspace*. Maxwell AFB, AL: Air University Press, 2007.

Conway, Maura. “Cyberterrorism: Hype and Reality.” In *Information Warfare*. Edited by Leigh Armistead. Washington DC: Potomac Books, 2007.

Dearth, Douglas H. and Charles A. Williams. "Information Age/Information War." In *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Edited by Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden. Fairfax, VA: AFCEA International Press, 1996.

Dearth, Douglas H. "The Human Factor in Future Conflict: Continuity and Change." In *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*. Edited by Alan D. Campen and Douglas H. Dearth. Fairfax, VA: AFCEA International Press, 2000.

De Cara, Chuck. "SOFTWARE & Grand Strategy: Liddell-Hart Updated." In *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* Edited by Alan D. Campen and Douglas H. Dearth. Fairfax, VA: AFCEA International Press, 2000.

Denma Translation Group. *The Art of War*. Boston & London: Shambhala Publications Inc, 2001.

Dictionary.com. <http://dictionary.reference.com>.

Douhet, Giulio. *Command of the Air*. Translated by Dino Ferrari. Washington DC: Coward-McCann Inc., 1983.

Fahrenkrug, Lt Col David T. *Cyberspace Defined*. On-line Air University Article. <http://www.maxwell.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html>.

Ghanea-Hercock, Robert. "The Art of Cyberwar." *SecurityPark.net*. 4 Feb 07. <http://www.securitypark.co.uk/article.asp?articleid=26620>.

Gouré, Daniel. "The Impact of the Information Revolution on Strategy and Doctrine." In *The Information revolution and National Security*. Washington DC: The Center for Strategic & International Studies, 1996.

Griffith, Samuel B. *Sun Tzu – The Art of War*. London, Oxford, New York: Oxford University Press, 1963.

Handel, Michael I. *Masters of War – Classical Strategic Thought*. London: Frank Cass Publishers, 1992.

Hashim, Ahmed. "Regional Powers and Information Warfare." In *The Information Revolution and National Security*. Washington DC: The Center for Strategic & International Studies, 1996.

Hosmer, Stephen T. "The Information Revolution and Psychological Effects" In *Strategic Appraisal: The Changing Role of Information in Warfare*. Santa Monica CA: RAND, 1999.

Iklé, Fred Charles. *Every War Must End*. New York NY: Columbia University Press, 1971.

- Jurich, Jon P. "Cyberwar and Customary International Law: The Potential of a "Bottom-up" Approach to an International Law of Information Operations" In *Chicago Journal of International Law*, Summer 2008.
- Kuehl, Dan. "Information Operations: The Policy and Organizational Evaluation." In *Information Warfare*. Edited by Leigh Armistead. Washington DC: Potomac Books, 2007.
- Libicki, Martin C. *Conquest in Cyberspace*. New York NY: Cambridge University Press, 2007.
- Libicki, Martin C. *Defending Cyberspace and Other Metaphors*. Washington DC: National Defense University, 1997.
- Libicki, Martin C. "The Small and the Many." In *In Athena's Camp*. Edited by John Arquilla and David Ronfeldt. Santa Monica, CA: Rand, 1997.
- Libicki, Martin C. *What is Information Warfare?* Washington DC: National Defense University, 1995.
- Libicki, Martin C. "Protecting the United States in Cyberspace." In *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Edited by Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden. Fairfax, VA: AFCEA International Press, 1996.
- Loescher, Michael. "The Information Warfare Campaign." In *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Edited by Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden. Fairfax, VA: AFCEA International Press, 1996.
- Lonsdale, David J. *The Nature of War in the Information Age*. London: Frank Cass, 2004.
- Malone, Jeff. "Speaking Out of Both Sides of Your Mouth: Approaches to Perception Management in Washington DC and Canberra." In *Information Warfare*. Edited by Leigh Armistead. Washington DC: Potomac Books, 2007.
- Marshall, Andrew W. "Forward." In *Strategic Appraisal: The Changing Role of Information in Warfare*. Edited by Zalmay M. Khalilzad and John P. White. Santa Monica CA: RAND, 1999.
- Michael, James Bret, Mikhail Auguston, Neil C. Rowe, and Richard D. Riehle. "Software Decoys: Intrusion Detection and Countermeasures." In *Proceedings of the 2002 IEEE Workshop on Information Assurance*, United States Military Academy, West Point NY, June 2002. http://www.cs.nps.navy.mil/people/faculty/bmichael/pubs/T2B2_IA2002_229.pdf.
- Nelson, Andrew H. *The Art of Information War*. Self Published, 1994-1995.
- Overy, Richard. *Why The Allies Won*. New York & London: W. W. Norton & Company, 1995.
- Pape, Robert A. *Bombing to Win*. Ithaca NY: Cornell University Press, 1996.

Pickett, George E. Jr. "Analogue to the Industrial Revolution." In *The Information Revolution and National Security*. Washington DC: The Center for Strategic & International Studies, 1996.

Rona, Thomas P. "From Scorched Earth to Information Warfare" In *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Edited by Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden. Fairfax, VA: AFCEA International Press, 1996.

Rothrock, John. "Information Warfare: Time For Some Constructive Skepticism?" In *In Athena's Camp*. Edited by John Arquilla and David Ronfeldt. Santa Monica, CA: Rand, 1997.

Rowe, Neil C. and Hy Rothstein. *Deception for Defense of Information Systems: Analogies From Conventional War*. Departments of Computer Sciences and Defense Analysis, U.S. Naval Postgraduate School. Monterey CA. <http://www.au.af.mil/au/awc/awcgate/nps/mildec.htm>.

Sawyer, Ralph D. *Sun Tzu – The Art of War*. Boulder CO: Westview Press, 1994.

Schwartzstein, Stuart J. D. "Introduction" In *The Information Revolution and National Security*. Washington DC: The Center for Strategic & International Studies, 1996.

Seaquist, Larry. "The Ten-Foot-Tall Electron: Finding Security in the Web." In *The Information Revolution and National Security*. Washington DC: The Center for Strategic & International Studies, 1996.

Sharp, Water, Gary, Sr. *Cyberspace and the Use of Force*, Falls Church VA: Aegis Research Corporation, 1999.

Shapiro, Jeremy. "Information and War: Is it a Revolution?" In *Strategic Appraisal: The Changing Role of Information in Warfare*, Edited by Zalmay M. Khalilzad and John P. White. Santa Monica CA: RAND, 1999.

Spitzner, Lance. *Honeypots: Definitions and Value of Honeypots*. 29 May 2003.
<http://www.tracking-hackers.com/papers/honeypots.html>.

Stein, George J. "Information Warfare." In *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Edited by Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden. Fairfax, VA: AFCEA International Press, 1996.

Szanfranski, Richard. "Neocortical Warfare? The Acme of Skill". In *In Athena's Camp*. Edited by John Arquilla and David Ronfeldt. Santa Monica, CA: Rand, 1997.

Thomas, Timothy, *Cyber Silhouettes – Shadows Over Information Operations*. Ft Leavenworth KS: Foreign Military Studies Officer, 2005.

Tinnel, Laura, O. Sami Saydjari and Dave Farrell. "Cyber Strategy and Tactics: An Analysis of Cyber Goals, Strategies, Tactics and Techniques." In *Proceedings of the 2002 IEEE Workshop*

on Information Assurance, United States Military Academy, West Point NY, June 2002.
http://www.cyberdefenseagency.com/publications/Cyberwar_Strategy_and_Tactics.pdf.

Weimann, Gabriel. *Terror on the Internet*. Washington, DC: United States Institute of Peace Press, 2006.

Wesson, Rick. To Noah Shachtman. "Air Force Aims to 'Rewrite Laws of Cyberspace'" *Wired Blog Network*, 4 Nov 2008. <http://blog.wired.com/defense/2008/11/air-force-aims.html>.

Woolsey, James R. "Resilience and Vulnerability in the Information Age" In *The Information Revolution and National Security*. Washington DC: The Center for Strategic & International Studies, 1996.